View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by Theseus

Opinnäytetyö (AMK)

Tietojenkäsittely

Yrityksen tietoliikenne ja tietoturva

2016

Joni Ketola

# BRING YOUR OWN DEVICE - MALLIN TIETOTURVARISKIT OPISKELIJAN NÄKÖKULMASTA

- Tapaus Turun ammattikorkeakoulu

TURUN AMMATTIKORKEAKOULU
TURKU UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖ (AMK) | TIIVISTELMÄ

TURUN AMMATTIKORKEAKOULU

Tietojenkäsittely | Yrityksen tietoliikenne ja tietoturva

Joulukuu 2016 | 32 sivua

Jarkko Paavola

Joni Ketola

# BRING YOUR OWN DEVICE -MALLIN TIETOTURVARISKIT OPISKELIJAN NÄKÖKULMASTA

## – Tapaus Turun ammattikorkeakoulu

Bring your own device (BYOD) on toimintatapa, jossa käyttäjät työskentelevät omilla laitteillaan organisaatiossa. Jokainen organisaatio on väistämättä siirtymässä BYOD-malliin jollain tavalla. Sen sijaan, että yritetään estää tätä ilmiötä tapahtumasta, IT-osastojen on tärkeä valmistautua ilmiöön varsinkin tietoturvariski ja –tietosuoja alueilla. Opinnäytetyön tavoitteena on selvittää BYOD-mallin tietoturvariskejä opiskelijan näkökulmasta. Lisäksi opinnäytteestä lukija saa perustietoa BYOD-mallista ja sen tuomista hyödyistä. Suurimpia BYOD-mallin hyötyjä on, että organisaatioiden kustannukset pienenevät sekä käyttäjien käyttömukavuus ja tehokkuus kasvavat.

BYOD-malli tarvitsee tuekseen erilaisia tekniikoita, joiden avulla turvallinen yhteyden muodostaminen organisaation dataan sekä järjestelmiin voidaan taata. Tällaisia tekniikoita on esimerkiksi työpöytävirtualisointi sekä erilaiset verkkosovellukset. Työpöytävirtualisoinnilla saadaan samanlainen käyttökokemus käytettävästä järjestelmästä tai laitteesta riippumatta. Verkkosovelluksilla asiakasohjelma muodostaa yhteyden selaimen avulla.

BYOD-mallin suurimpia haasteita ovat sen tuomat tietoturvariskit, joita IT-osastot pyrkivät minimoimaan. Tietoturvauhkia ja hyökkäyksiä vastaan taistellaan muun muassa teknisillä toimilla, jotka ovat ennaltaehkäisy, havaitseminen ja reaktio. Nämä vastatoimet ovat kytköksissä keskenään, ja niitä muutetaan jatkuvasti järjestelmässä syntyvien tapahtumien myötä.

Turun ammattikorkeakoulun IT-asiantuntijoille pidettiin fokusryhmähaastattelu. Haastattelun tavoitteena oli selvittää heidän näkemyksiään BYOD-mallin tuomista tietoturvariskeistä. Haastattelussa tunnistetut tietoturvariskit olivat pitkälti samanlaisia, kuin mitä kirjallisuudesta löytyi. Suurimmat tietoturvariskit syntyvät käyttäjien tekemistä virheistä ja päivittämättömistä laitteista.

ASIASANAT:

Bring your own device, BYOD, tietoturvariski

BACHELOR´S THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Business Information Technology | Business Data Communications and Information Security

December 2016 | 32 pages

Jarkko Paavola

Joni Ketola

# INFORMATION SECURITY RISKS OF BYOD FROM STUDENT'S POINT OF VIEW

## – Case Turku University of Appied Sciences

Bring your own device (BYOD) is a policy, where users work with their own devices in an organization. Every organization is inevitably moving towards BYOD in some way. Instead of trying to stop this phenomenon from happening, IT-departments need to prepare for it, especially in information security and data protection areas. The objective of this thesis is to examine the information security risks of BYOD from student's point of view. In addition reader gets basic information about BYOD and learns about the benefits that it brings. The biggest advantages of BYOD are the decrease of costs in an organization and increase in the ease of operation and efficiency.

In order to establish a secure connection to organizations data and systems, BYOD needs different kind of techniques to support it. These techniques are for example desktop virtualization and different kind of web applications. Desktop virtualization gives the same user experience, despite the system or device used. With web applications, a client connects through a browser.

The biggest challenges of BYOD are the information security risks that it brings, which IT-departments are trying to minimize. Among other things, information security threats and attacks are fought against with technological countermeasures which are prevention, detection and reaction. These countermeasures are related to each other and they are changed constantly depending on events in systems.

IT-specialists of Turku University of Applied Sciences were conducted in a focus group interview. The objective of the interview was to find out their opinions about the information security risks that comes with BYOD. The results of the interview were more or less the same than what is mentioned in literature. The biggest information security risks come from mistakes that users make and unpatched equipment.

KEYWORDS:

Bring your own device, BYOD, information security risk

# SISÄLTÖ

# KUVAT



# KUVIOT



# TAULUKOT

# KÄYTETTY SANASTO

| | |
|---|---|
| basic input-output system | tietokoneohjelma, joka lataa käyttöjärjestelmän keskusmuistiin käynnistyksen yhteydessä |
| bugi | sovelluksessa tai järjestelmässä oleva ohjelmointivirhe |
| asiakasohjelma | ohjelma, jolla luodaan yhteys serverin tarjoamaan palveluun |
| hybridisovellus | verkkosovellus, joka asennetaan erikseen laitteeseen, mutta vaatii kuitenkin verkkoyhteyden toimiakseen |
| hypertext transfer protocol secure | protokolla, jota käytetään datan suojaamiseen verkossa |
| virtual private network | tapa, jolla yksityisien verkkojen välille muodostetaan turvallinen yhteys julkisen verkon kautta |
| key logger-hyökkäys | näppäimistön painalluksia seuraava ohjelma, joka tallentaa ja lähettää tiedot ulkopuoliselle henkilölle |
| sniffing | passiivinen hyökkäysmuoto, jossa seurataan verkossa olevia tapahtumia ja hankitaan käyttäjästä tietoja |
| use what you are told | käyttäjä käyttää laitteita, jotka hänelle määrätään |
| virtual desktop infrastructure | virtualisointitekniikka, jossa työpöydät ja data sijaitsevat servereillä |
| Wi-Fi | tekniikka, jonka avulla laite yhdistetään lähiverkkoon langattomasti |
| wireless local area network | langaton lähiverkko |

# 1 JOHDANTO

Tämän opinnäytetyön aiheena on Bring your own device -malli (BYOD) ja sen tuomat tietoturvariskit opiskelijoiden näkökulmasta. BYOD-malli on yleistyvä trendi ympäri maailmaa. Jokaisessa organisaatiossa ollaan väistämättä siirtymässä siihen ainakin jollain tapaa. Sen sijaan että yritettäisiin estää ilmiötä tapahtumasta, on tärkeämpää varautua ja valmistautua BYOD-malliin. BYOD on käsite, jossa käyttäjät pääsevät omilla laitteillaan käsiksi organisaation dataan ja järjestelmiin (IBM 2016). Suurin haaste on tietoturva-asioissa. Opinnäyteaihevalinta oli helppo, sillä se on ajankohtainen. Myös kiinnostus tieturva ja -suoja asioista edesauttoivat valintaa. Opinnäytetyön toimeksiantajana on Turun ammattikorkeakoulu. Ammattikorkeakoululla on jo valmiiksi suuri osa datasta verkossa, joten BYOD-malliin siirtyminen on luontevaa.

Aluksi opinnäytteessä käsitellään BYOD-mallia yleisellä tasolla ja pohditaan sen tuomia hyötyjä ja etuja Turun ammattikorkeakoululle. Sitten tarkastellaan BYOD-mallin tuomia uhkia ja tietoturvariskejä sekä tehdään riskienhallinta-analyysia. Lopuksi analysoidaan fokusryhmähaastattelua, johon ammattikorkeakoulun IT-asiantuntijat osallistuivat.

Opinnäytteen tavoitteena on selvittää opiskelijan näkökulmasta BYOD-mallin tietoturvariskien lisäksi sitä, mitä asioita BYOD-mallia käytettäessä tulee ottaa huomioon. Toinen tavoite on antaa lukijalle peruskäsitys siitä, mitä BYOD-malli tarkoittaa. Vaikka tämä työ tehdään Turun ammattikorkeakoululle, sitä voi hyvin soveltaa myös muissa organisaatioissa. Tutkimusmenetelmänä on tapaustutkimus.

# 2 BRING YOUR OWN DEVICE

Bring your own device on käsite, joka tarkoittaa, että käyttäjät voivat omilla laitteillaan, kuten kannettavilla tai älypuhelimilla, päästä käsiksi organisaation dataan ja järjestelmiin. BYOD-käsite tuli esille ensimmäisen kerran vuonna 2009 Intelin toimesta. Vuonna 2011 BYOD-malli yleistyi, kun Unisys ja Citrix Systems toivat julkisuuteen omat näkökulmansa aiheesta. Mobiililaitteiden yleistymisen myötä omia laitteita käytetään koko ajan enemmän organisaatioissa. Tämä lisää paineita IT-osastoilla, sillä käyttäjien yksityisyys täytyy voida turvata sekä varmistaa, että organisaation arkaluontoinen data ei pääse vuotamaan. (Prashant ym. 2013, 1.)

BYOD-mallin myötä IT-osastot ja -johtajat joutuvat suunnittelemaan sekä toteuttamaan uusia toimintamalleja, jotka kattavat tukemattomien laitteiden hallinnan. Verkon turvallisuus on tärkein. Mark Coates, Good Technologyn varajohtaja, kiteyttää BYOD-mallin toteuttamisen kolmeen eri vaiheeseen. Kaikki alkaa turvallisesta laitehallinnasta. Oli kyseessä sitten käyttäjän itsensä hankkima laite tai organisaation tarjoama. Toisessa ja kolmannessa vaiheessa keskitytään mobiilisovelluksiin ja dataan. Aluksi etsitään toimintaan sopivat sovellukset ja otetaan ne käyttöön. Sen jälkeen muodostetaan turvallinen sovellusten välinen yhteys, jossa liikkuvuus tuo suurimman edun. (Evans 2015.)

## 2.1 Mobiililaitteet

Mobiililaitteita on vaikea määritellä, sillä ne kehittyvät ja niiden ominaisuudet muuttuvat jatkuvasti. Yleisimpiä tunnusomaisia piirteitä mobiililaitteilla on kuitenkin pienikokoisuus, paikallinen muisti, kovalevy, mikrofoni, kaiuttimet, kamera, käyttöjärjestelmä sekä erilaiset sovellukset. Lisäksi mobiililaitteilla on vähintään yksi langaton verkkoliitäntä. Verkkoliitäntä käyttää joko Wi-Fi-yhteyttä, matkapuhelinverkkoa tai jotain muuta teknologiaa muodostaakseen yhteyden internettiin. (Jackson 2013.)

Cisco Internet Business Solution Groupin, vuonna 2012 tekemän tutkimuksen mukaan, 78 % toimistotyöntekijöistä ilmoitti käyttävänsä kannettavaa, älypuhelinta, tablettia tms. työasioidensa hoitamiseen. 65 % osallistujista ei pystyisi tekemään töitään ilman mobiililaitteita. Tietotyöntekijöistä 44 % teki etätöitä vähintään kerran viikossa. Tutkimuksesta saatujen tietojen mukaan etätyö säästää yrityksille 2 500 dollaria vuodessa per työntekijä. (Barbier ym. 2012, 1.)

## 2.2 Työpöytävirtualisointi

BYOD ja työpöytävirtualisointi ovat hyvin pitkälti kytköksissä keskenään. Työpöytävirtualisoinnin avulla saadaan samanlainen käyttökokemus käytössä olevasta järjestelmästä tai laitteesta huolimatta. (Barbier ym. 2012, 1, 3.) Työpöytävirtualisoinnilla voidaan viitata useisiin teknologioihin. Ne vaihtelevat kuluttajakeskeisistä etätyöpöytäsovelluksista, joilla käyttäjä voi luoda yhteyden kotikoneeseen, suuryritystason VDI-järjestelmiin (virtual desktop infrastructure), joilla virtuaaliset työpöydät sekä data sijaitsevat servereillä. Työpöytävirtualisointi on yksi tapa, jolla voidaan hallita tietoturvaa ja minimoida riskejä. (Endler 2013.)

DaaS (desktop-as-a-service) tuo virtuaalisen työpöydän käyttäjille pilven kautta. Tällöin käyttäjä tarvitsee ainoastaan internetyhteyden voidakseen hoitaa työtehtäviään laitteesta riippumatta. DaaS poistaa paikallisten laitteiden hallinnoinnin ja siirtää vastuun ulkoiselle palveluntarjoajalle. Kustannukset pienentyvät sekä IT-osastojen työtaakka laskee. Pilviteknologian suosion kasvaessa DaaS on noussut yhdeksi suosituimmaksi virtualisointitavaksi. (ITGCT 2015.)

## 2.3 Verkkosovellus

Verkkosovellukset ovat tärkeitä mobiililaitteille, koska asiakasohjelma käyttää tavallista selainta, joka soveltuu kaikkiin alustoihin. Kaikki organisaatiot käyttävät verkkosovelluksia jollain tapaa. Jos yhteys luodaan HTTPS-yhteydellä (hypertext

transfer protocol secure), ei ole pakko luoda VPN-yhteyttä (virtual private network). Kuitenkin verkkosovellukset toimivat internetin välityksellä, joten jonkinlaiset suojausmenetelmät ovat pakollisia, jotta datan eheys voidaan taata. Verkkosovelluksilla voidaan tukea suuria määriä laitteita edullisesti. Kaistanleveyden ei tarvitse olla korkea, sillä yhteys voidaan muodostaa WLAN-yhteyden (wireless local area network) lisäksi myös matkapuhelinverkoilla. (Disterer & Kleiner 2013, 6.)

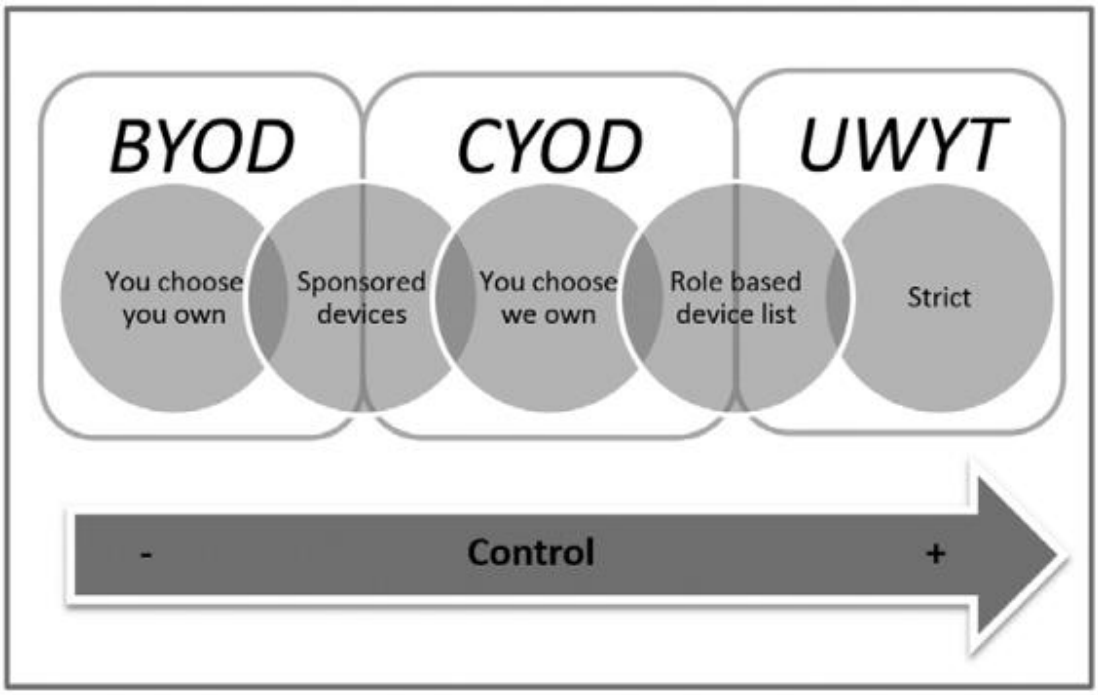
Selaimilla on pääsy paikalliseen järjestelmään. Kun esimerkiksi sivuhistoria tallentuu laitteeseen, se tuo omat tietoturvariskinsä, kuten laitteen saastuminen haittaohjelmilla. Verkkosovelluksia käytettäessä laitteet ovat koko ajan yhteydessä verkkoon. Offline-tilassa ei voi työskennellä, ellei data ole valmiiksi tallennettuna laitteeseen. Jos käytettävä data on laitteessa, puhutaan niin sanotusta hybridisovelluksesta. (Disterer & Kleiner 2013, 6–7.)

## 2.4 Choose your own device

Choose your own device -malli on hyvin samankaltainen kuin BYOD. Sen sijaan, että käyttäjät itse hankkisivat laitteensa, he voivat valita ennalta määrätyistä laitteista haluamansa laitteet, jotka organisaatio hankkii heille käytettäväksi. Tällä tavoin laitteiden skaala saadaan pienemmäksi, ja niitä on helpompi kontrolloida. Laitteiden ollessa organisaation omistuksessa niiden käyttöön voidaan vaikuttaa enemmän ja valvonta on helpompaa. (Brodin 2016, 4.)

Kuvassa 1 näkyy kuinka organisaation kontrolli kasvaa laitteidenhallinnassa siirryttäessä BYOD:stä kohti UWYT:tä (use what you are told). Vasemmalta oikealle katsottuna strategiat ovat

- käyttäjä valitsee ja omistaa
- sponsoroidut laitteet
- käyttäjä valitsee ja organisaatio omistaa
- roolipohjaiset laitelistat
- ennalta määrätyt laitteet.




Kuva 1. Organisaation kontrolli verrattuna eri mobiililaitestrategioihin. (Brodin 2016, 2).

## 2.5 BYOD-mallin hyödyt

BYOD-mallista on paljon hyötyjä:

- Organisaation kustannukset vähenevät.
- Käyttömukavuus ja tehokkuus lisääntyvät.
- Käyttäjien etätyöskentely helpottuu.
- Omista laitteista pidetään parempaa huolta. (Prashant ym. 2013, 2.)

Kustannuksia saadaan vähennettyä, kun organisaation ei tarvitse käyttää niin paljon resursseja laitteistohankintoihin. Myös lisenssikustannukset saattavat pienentyä, sillä käyttäjät hankkivat omia sovelluksia laitteisiinsa. Virtualisoinnin avulla organisaatiot eivät tarvitse niin suuria fyysisiä tiloja, sillä esimerkiksi myyntiedustajat voivat työskennellä täysin etänä. (Swanepoel 2015, 1.)

Ciscon vuonna 2012 julkaiseman tutkimuksen mukaan organisaatiot, joilla on BYOD-malli käytössä, ovat muita organisaatioita houkuttelevampia. Tällaiset

organisaatiot säilyttävät myös lahjakkaimmat työntekijänsä muita paremmin. Ilmiö näkyi varsinkin nuorten työnhakijoiden tilastoissa. (Swanepoel 2015, 1.)

Mobiililaitteiden käyttö BYOD-mallissa edesauttaa käyttäjiä heidän työtehtäviensä suorittamisessa, sillä he voivat tehdä niitä missä ja milloin vain. Esimerkiksi vakuutusneuvoja voi helposti yhdistää tabletillaan yrityksen dataan, kun hän on konsultointitilanteessa asiakkaan kanssa. Liikkuvuuden lisäksi tutut laitteet sekä omat laitemieltymykset lisäävät työntekijöiden tuottavuutta ja tehokkuutta. Oikein suunniteltu BYOD-malli voi tuoda organisaatiolle suuren kilpailuedun. (Swanepoel 2015, 1.)

# 3 TIETOTURVARISKIT

Tietoturvariskillä tarkoitetaan organisaation voimavaran menettämisen mahdollisuutta, mikä todennäköisesti tapahtuu, jos jokin uhka pystyy hyväksikäyttämään haavoittuvuutta. Tietoturvariskeistä puhuttaessa tulee ottaa huomioon monia avaintekijöitä. Tärkeintä on kuitenkin miettiä, mistä riskit johtuvat ja miten ne näkyvät. Tietoturvariskejä voidaan lähestyä monella eri tavalla, mutta ne kaikki kuvaillaan joko määrällisiksi eli kvantitatiivisiksi tai laadullisiksi eli kvalitatiivisiksi lähestymistavoiksi. (Landoll 2011, 30–31.)

### Kvantitatiivinen lähestymistapa

Kvantitatiivinen lähestymistapa luottaa tietynlaisiin kaavoihin ja laskelmiin, joilla määritetään tietoturvariskin suuruus. Kvantitatiivisen lähestymistavan etuna on se, että tutkimuksista saaduilla tiedoilla voidaan näyttää riskien suuruus rahallisella tasolla. Tämän kaltaiset laskelmat voivat kuitenkin olla suhteellisen monimutkaisia. Myös muuttujien tarkat arvot voi olla vaikea hankkia, kun käytetään kvantitatiivisia kaavoja. (Landoll 2011, 31.)

### Kvalitatiivinen lähestymistapa

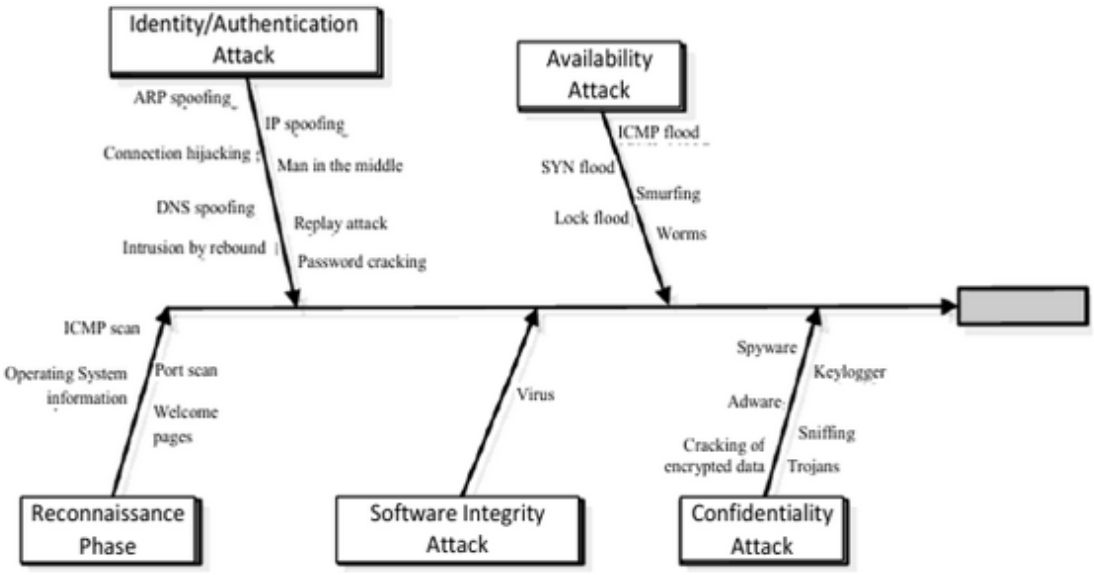
Kvalitatiivinen lähestymistapa on taas subjektiivinen. Voimavarojen arviointi, uhat, haavoittuvuudet ja tietoturvariskit koostuvat jonkun omaan näkemykseen, ja eivät näin ollen ole yleispäteviä. Kvalitatiivista lähestymistapaa käytettäessä tutkimustulokset ovat helpommin ymmärrettävissä, ja usein myös organisaation tietoturvariskeihin liittyen tarkoituksenmukaisemmat. Haittapuolena kvalitatiivisessa lähestymistavassa on se, että tulokset perustuvat tutkijan omaan näkemykseen. Siitä syystä esimerkiksi hallinnollisissa asemissa olevat henkilöt eivät välttämättä luota niihin. (Landoll 2011, 31.)

## 3.1 Uhat ja hyökkäykset

On mahdotonta listata kaikkia mahdollisia hyökkäyksiä, joita mobiililaitteisiin tehdään, sillä niitä on sadoittain ja uusia kehitetään koko ajan. Seuraavaksi tarkastellaan hyökkäyksissä käytettyjä yleisimpiä tekniikoita ja tapoja, jotta nämä uhat voidaan määrittää ja ottaa käytäntöön asianmukaiset suojausmenetelmät. (Assing & Calé 2013, 7.)

Kuviossa 1 tietoturvahyökkäykset on jaoteltu viiteen eri luokkaan, joita ovat

- Reconnaissance phase, joka tarkoittaa tekniikoita, joilla hakkeri voi kerätä tietoja kohteestaan ennen hyökkäyksen aloittamista.
- Identity/Authentication Attack, joka tarkoittaa tekniikoita, joilla hakkeri voi varastaa laitteen, ohjelman tai käyttäjän identiteetin voidakseen käyttää olemassa olevia käyttöoikeuksia.
- Software Integrity Attack, joka tarkoittaa tekniikoita, joilla hakkeri voi kaapata tai muuttaa ohjelmien toimintoja niin, että ne suorittavat hakkeria hyödyntäviä tehtäviä.
- Availability Attack, joka tarkoittaa tekniikoita, joilla hakkeri voi häiritä tai kokonaan keskeyttää kohteen palveluita.
- Confidentiality Attack, joka tarkoittaa tekniikoita, joilla hakkeri saa haltuunsa informaatioita, mikä ei muutoin ole saatavilla.




Kuvio 1. Eri hyökkäysmuotojen luokat. (Assing & Calé 2013, 8).

Yksi hyökkäys voi tehdä moneen eri luokkaan kuuluvia asioita. Esimerkiksi troijalainen voi aluksi kerätä tietoa järjestelmästä, jonka jälkeen se varastaa ylläpitäjän salasanan, ja sen jälkeen formatoi kovalevyn. (Assing & Calé 2013, 7–8.)

Omien laitteiden tuominen organisaatioon tuo mukanaan paljon haasteita. Ne voivat hävitä tai tulla varastetuksi, jolloin myös henkilökohtaiset tiedot ovat uhattuna. Mobiililaitteissa on suuri määrä erilaisia käyttöjärjestelmiä ja ne vanhentuvat nopeasti. Lisäksi mobiililaitteet on rakennettu erilaisille alustoille. Tietoturva ja -suoja ei välttämättä ole laitteissa riittävällä tasolla. Tällaisia puutteita ovat esimerkiksi

- virusturva
- palomuuri
- sovelluspäivitykset
- konfigurointiasetukset. (Prashant ym. 2013, 2.)

Kun organisaatiolla ei ole enää omat laitteet käytössä, on vaikea tasapainoilla täsmällisen tietoturvan ja henkilökohtaisen datan välillä. Kadonneisiin tai varastettuihin laitteisiin ei kiinnitetä niin paljon huomioita, kun ne eivät ole enää

organisaation omistuksessa. IT-osastot eivät saa tapauksista edes tietoa, jos käyttäjä itse ei tee ilmoitusta. Luottamuksellista dataa liikkuu turvattomilla kanavilla, joka on helposti kaapattavissa. Lisäksi mobiililaitteet ovat yleensä aina yhdistettynä verkkoon, ja niistä voidaan tehdä myös tukiasemia. (Prashant ym. 2013, 2.)

## 3.2 Tekniset vastatoimet

Teknisellä vastatoimella tarkoitetaan prosessia, mikä siirtyy eri vaiheissa rakentaen ja vahvistaen itseään. Strategioita ja menetelmiä on monenlaisia, mutta ne kaikki voidaan jakaa kolmeen eri vaiheeseen, jotka ovat

- ennaltaehkäisy
- havaitseminen
- toiminta.

Yhden vaiheen tehtyä tarvittavat toiminnat prosessissa siirrytään taas seuraavaan vaiheeseen. Jatkuva uusien tietoturvauhkien ja hyökkäysten kasvu edellyttää myös vastatoimien metodien jatkuvaa säätöä. Muutos jossain näistä kolmesta vaiheesta vaikuttaa koko prosessin sykliin jollain tavalla. Esimerkiksi toimintavaiheessa olleet tapahtumat vaikuttavat ennaltaehkäisyn uusiin suunnitelmiin ja havaitsemisen konfigurointeihin. (La Piedra 2002, 2.)

Ennaltaehkäisyn, havaitsemisen ja toiminnan kaltaisessa suojauksessa täytyy myös ymmärtää kolme merkittävää seikkaa.

- Mikään puolustus ei ole läpäisemätön. Tietojärjestelmien suojauksien toteutuksessa ei saa olla liian itsevarma sen toimivuudesta.
- Koko turvajärjestelmä ei saa tuhoutua yhden suojakerroksen ollessa poissa käytöstä tai murtuessa. Tämä heijastuu varsinkin syvemmän suojauksen järjestelmiin, joita esimerkiksi puolustusvoimat käyttää.
- Suojausmallin täytyy viivyttää hyökkääjää mahdollisimman pitkään, jotta tämä ei saavuttaisi päämääräänsä. Samaan aikaan puolustuksen tulee

havaita hyökkääjä mahdollisimman nopeasti, jotta voidaan alkaa vastatoimiin. (Assing & Calé 2013, 66.)

### 3.2.1 Ennaltaehkäisy

Laitteiden ollessa organisaation verkkoon yhdistettynä ne ovat suojattuna organisaation turvajärjestelmien ja toimintamallien takana. Näin ei kuitenkaan ole, kun laitteet yhdistetään tietojärjestelmiin etänä. Ennaltaehkäisyssä täytyy ottaa huomioon mobiililaitteet itsenään sekä data, johon laitteet tarvitsevat pääsyn. Laitteiden suojaus koostuu pääasiassa siihen vaikuttavien haavoittuvuuksien hallinnasta. Datan suojaus taas vaatii laitteissa olevan datan salaustekniikoita. (Assing & Calé 2013, 66–67.)

**Mobiililaitteiden suojaus**

Hakkerit käyttävät hyväkseen bugeja etsiessään haavoittuvuuksia. Samaan aikaan ohjelmistokehittäjät yrittävät paikata näitä erilaisilla sovellus- tai järjestelmäpäivityksillä eli patcheillä. Käyttäjien onkin syytä päivittää kaikki sovellukset ja laitteet aina, kun päivityksiä on saatavilla. Mobiililaitteet ovat erityisesti uhattuna, sillä ne eivät ole suojattuna organisaation turvajärjestelmillä, kuten palomuurilla. (Assing & Calé 2013, 67.)

Käyttäjien pitäisi lukita ja suojata laitteet vahvoilla salasanoilla aina silloin, kun niitä ei käytetä. Näytönsäästäjä on hyvä olla käytössä, sillä lukkiutumisen lisäksi näytönsäästäjä säästää myös laitteen virtaa. Lukitsemalla laitteet estetään muita käyttämästä laitteita, jos ne jäävät hetkeksi vartioimatta. USB-porttien kautta voidaan siirtää nopeasti suuria määriä dataa. USB-2.0 voi siirtää 480 Mbit/s ja USB-3.0 jopa 5000 Mbit/s. Tämän vuoksi laitteen data on nopeasti kopioitu, jos se jätetään hetkeksi vartioimatta. Luotettavan datan lisäksi käyttäjien henkilökohtainen data on vaarassa. Yksi tapa estää tämän kaltainen riski on kytkeä USB-portit pois käytöstä. Se voi kuitenkin osoittautua hankalaksi, sillä

suurin osa oheislaitteista kytketään USB-porttien kautta laitteeseen. (Assing & Calé 2013, 70–71.)

**Datan suojaus**

Vuonna 2009 BT Groupin tutkijat ostivat 300 kovalevyä eBay:stä. Tutkimustulostensa perusteella he huomasivat, että 34 % kovalevyistä sisälsi henkilökohtaista tai arkaluontoista dataa. Kovalevyissä oli muun muassa tietoturvalokeja Ranskan suurlähetystöstä sekä ohjeita, kuinka torjua Irakin scud ohjuksia. Vanhoja laitteita hävitettäessä tai myydessä käyttäjien on hyvä muistaa, että pelkkä kovalevyn tyhjentäminen ei välttämättä poista dataa kokonaan ennen, kuin sen päälle on kirjoitettu jotain muuta. Turvalliseen datan poistoon on olemassa sitä varten tehtyjä sovelluksia, jotka on syytä suorittaa ennen laitteiden hävittämistä. (Assing & Calé 2013, 72.)

Melkein jokaiseen mobiililaitteeseen voi kytkeytyä etänä, jos käyttäjä on laittanut mobiililaitteen asetukset oikein. Laitteen tullessa varastetuksi tai hävitessä käyttäjä voi pyyhkiä laitteen tiedot etänä. Tämä tietysti edellyttää, että hävinnyt tai varastettu laite on kytkettynä verkkoon. (Assing & Calé 2013, 80.)

Yleisissä tiloissa ei välttämättä haluta näyttää muille ympärillä oleville laitteen näytössä näkyviä tietoja. Jotkut yritykset ovat kehittäneet siihen tarkoitukseen näyttöön kiinnitettäviä näyttösuodattimia. On myös sovelluksia, joilla voidaan säätää, miten hyvin laitteen ympärillä olevat ihmiset voivat nähdä näytössä olevia tietoja. Näyttösuodattimet esimerkiksi pienentävät kulmaa, josta näytön voi nähdä. Yksi tapa on tietysti olla selkä seinää vasten, jotta muut eivät näe laitteen tietoja. (Assing & Calé 2013, 80.)

### 3.2.2 Havaitseminen

Tietoturvauhkien ja -haavoittuvuuksien havaitseminen on tärkeää alati kasvavissa uhkien ympäristössä. Ei ole olemassa läpäisemätöntä turvaratkaisua. Suojausjärjestelmä on syytä ottaa käyttöön niin, että kun yksi taso pettää, siitä

lähetetään hälytys. Samaan aikaan seuraavat tasot suojaavat järjestelmää. Erilaiset tunkeilijan havaitsemisjärjestelmät (intrusion detection system) on suunniteltu tähän tarkoitukseen. Tunkeilijan havaitsemisjärjestelmät valvovat järjestelmää, ja ilmoittavat vastuussa oleville henkilöille, kun järjestelmässä olevat tapahtumat vaativat tutkimista. Tunkeilijan havaitsemisjärjestelmät havaitsevat muun muassa hyökkäysallekirjoitukset, tiedostomuutokset, konfiguroinnit ja aktiivisuuden. Havaitsemistyökalut on hyvä sijoittaa verkko- ja sovellustasoille. (La Piedra 2002, 5.)

### 3.2.3 Toiminta

Viimeisin suojauksen taso, kun uhka on havaittu, on toiminta. Käytännössä tämä tarkoittaa, että valitaan sopivat metodit, joilla uhka eristetään ja tuhotaan. (Assing & Calé 2013, 95.) Seuraavaksi tarkastellaan eri työkaluja, millä havaitaan ja toimitaan erilaisia uhkia vastaan.

**Palomuuri**

Palomuuri on suojalaite, joka suodattaa yhteyksiä eri verkkojen välillä. Suodattaminen tapahtuu perinteisesti IP-osoitteen lähteestä ja päämäärästä. Palomuuri ottaa myös huomioon, minkä portin kautta tiedon täytyy kulkea. Konfiguroinneista riippuen palomuuri joko päästää tai evää yhteyden verkkojen välillä. Lisäksi riippuen laitteen teknisyydestä, voidaan ottaa käytäntöön erilaisia palomuurisääntöjä, kuten protokolla tyyppi. Tietoturvasyistä käyttäjiä ei kuitenkaan suositella muuttamaan konfigurointeja, jos näihin asioihin ei ole perehtynyt. (Assing & Calé 2013, 95, 100.)

Sen lisäksi, että organisaatioilla on omat palomuurijärjestelmänsä, pitää käyttäjillä olla laitteissaan myös oma. On olemassa pääasiassa kahdenlaisia henkilökohtaisia palomuureja. Palomuuri voi olla sovellus, joka on asennettuna tietokoneeseen. Toinen vaihtoehto on ulkoinen laitteisto esimerkiksi reititin, jolla on omat suodattamistoiminnat. Jos palomuuri on asennettuna tietokoneeseen,

on kyseessä yleensä jonkinlaisesta asennuspaketista, jonka mukana tulee myös haittaohjelmien torjunta-sovellus. Tämän kaltaiset tuotepaketit ovat kehittyneet huomattavasti, ja niitä tarjotaan myös yrityskäyttöön. (Assing & Calé 2013, 100.)

**Haittaohjelmien torjunta-sovellus**

Haittaohjelmien torjunta-sovelluksella on merkittävä rooli taistelussa viruksia vastaan. Pelkkä haittaohjelmien torjunta-sovellus ei kuitenkaan riitä suojaamaan laitteita viruksilta, vaan lisäksi tarvitaan muita suojausmenetelmiä, kuten palomuuri. Haittaohjelmien torjunta-sovelluksilla on kaksi funktiota. Ensimmäinen on tartuntojen havaitseminen ja analysointi. Toinen on saastuneiden tiedostojen korjaaminen tai karanteeniin siirtäminen. (Assing & Calé 2013, 104.)

Haittaohjelmia havaitaan joko staattisesti tai dynaamisesti. Staattisesti viruksia havaittaessa sovelluksella on käytössä tietokanta, jonka avulla sovellus tunnistaa yleisimmät virukset järjestelmästä. Haittapuolena on, että virukset voivat muuttua tai niiden koodia voidaan muokata. Tällöin sovellus ei enää tunnista viruksia ennen kuin tietokanta on päivitetty. Toinen staattinen tapa on heuristinen metodi. Siinä epätavallista käyttäytymistä etsitään analysoitavista ohjelmista liittyen esimerkiksi sääntöihin tai strategioihin. Tämän lähestymistavan vaikeuksia on, että tulokset voivat olla niin sanottuja vääriä positiivisia. Hakkerit myös analysoivat näitä sääntöjä voidakseen kiertää ne. Viruksien dynaaminen havaitseminen tarkoittaa, että manuaalisesti käsketään haittaohjelmien torjunta-sovellusta etsimään jotain rajattua aluetta tai sovelluksia virusten varalta. Dynaamisia tekniikoita käytetään yleensä vain tarvittaessa, sillä ne kuluttavat suuria määriä tehoa haitaten laitteen suorituskykyä. (Assing & Calé 2013, 104–105.)

## 3.3 Tunnistaminen ja todentaminen

Tunnistaminen ja todentaminen ovat jokaisen tietojärjestelmän kulmakivi. Näillä mekanismeilla käyttäjä voidaan tunnistaa sekä antaa hänelle pääsy resursseihin,

joihin hänellä on oikeudet. Riippumatta siitä, millaista menetelmää kulunvalvonnassa käytetään, todentaminen perustuu johonkin seuraavista kolmesta menetelmästä.

- Mitä sinä tiedät – käyttäjän täytyy voida todistaa tietävänsä jotain salaista tietoa, kuten salasana.
- Mitä sinulla on – käyttäjällä täytyy olla hallussaan jokin esine, kuten avain tai kulkukortti.
- Kuka sinä olet – käyttäjä omaa jonkin tunnusomaisen piirteen, kuten puheen ääni tai sormenjälki. (Assing & Calé 2013, 139–140.)

Etäyhteyttä käytettäessä kulunvalvonnan täytyy olla tiukempaa, kuin organisaation tiloissa olevissa laitteissa. Käyttäjien omat mobiililaitteet lisäävät tietoturvariskejä, sillä niitä käytetään työasioiden lisäksi myös omiin tarkoituksiin. Epäilyttävät verkkosivustot, kuten aikuisviihdesivustot voivat helposti saastuttaa laitteen. Laitteissa voi olla myös vanhentuneet sovellus- tai järjestelmäpäivitykset. (Assing & Calé 2013, 138.)

**Staattinen salasana**

Staattinen salasana on yksi vanhimmista todentamismenetelmistä. Kun käyttäjä on tunnistanut itsensä, häneltä kysytään salasana. Tätä todentamismenetelmää käytettäessä täytyy salasanojen turvallisuuspolitiikka määrittää tarkasti. Seuraavassa luetelmassa on erilaisia vaihtoehtoja salasanojen määrityksistä, kuten

- salasanan voimassaoloaika
- yritysten määrä ennen kuin tili suljetaan
- kirjainten minimimäärä
- kirjaintyyppien minimimäärä (numerot, erikoismerkit, jne.)
- kiellettyjen sanojen lista
- tilin lukkiutuminen sen oltua käyttämättömänä ennalta määrätyn periodin

- kriteerit poikkeavien todentamisien kontrollointiin. (Assing & Calé 2013, 140–141.)

Taulukossa 1 on esitettynä, kuinka paljon erilaisten kirjainten käyttäminen salasanoissa vaikuttaa. Taulukko on laskettu kahdeksan kirjaimen mukaan. Keskimmäisessä sarakkeessa näkyy, mitä erilaisia kirjaimia on käytetty. Oikeassa sarakkeessa on kaikki mahdolliset eri salasanayhdistelmävaihtoehdot.

Taulukko 1. Salasanan vahvuus suhteessa käytettyihin kirjaimiin. (Assing & Calé 2013, 140).

| Length of password | Characters used | Number of combinations |
|---|---|---|
| 8 | Alphabetic (a-z) | 208,827,064,576 |
| 8 | Alphanumeric (a-z + 0-9) | 2,821,109,907,456 |
| 8 | Alphanumeric with lower and upper case (a-z + A-Z + 0-9) | 218,340,105,584,896 |
| 8 | Alphanumeric with lower and upper case and 20 special characters (a-z + A-Z + 0-9 + &-@) | 2,044,140,858,654,976 |

Käyttäjien on tärkeää ymmärtää, että mitä pidempi ja monimutkaisempi salasana on, sitä turvallisempi ja vaikeampi se on hakkerien murtaa. (Assing & Calé 2013, 142.)

### Dynaaminen salasana

Dynaaminen salasana perustuu siihen, että todentamiseen käytettävä koodi on voimassa vain kerran. Jokaisen uuden yhteyden muodostamiseen käyttäjän täytyy generoida uusi salasana. Tämänlainen järjestelmä yhdistää todentamismenetelmät *mitä sinulla on* ja *mitä sinä tiedät*. Käyttäjä voi vastaanottaa esimerkiksi puhelimeensa tekstiviestin, joka sisältää kertakäyttöisen kirjautumistunnuksen. Dynaaminen salasana suojaa erityisesti key logger -hyökkäyksiltä ja tietojen kalastelulta (sniffing). (Assing & Calé 2013, 144–145.)

# 4 HAASTATTELU AMMATTIKORKEAKOULUN IT-ASIANTUNTIJOILLE

Turun ammattikorkeakoulun IT-asiantuntijoille pidettiin fokusryhmähaastattelu. Fokusryhmämetodia käytetään, jotta saadaan syvempää tietoa yksilöiden asenteista, käsityksistä, uskomuksista ja mielipiteistä liittyen johonkin spesifiin aiheeseen. Fokusryhmän tavoitteena on saada osallistujat keskustelemaan keskenään haastattelijan ohjatessa keskustelua kysymyksillään. Osallistujien määrä tyypillisesti vaihtelee seitsemästä kymmeneen. (Marczak & Sewell 2016.)

Valitsin fokusryhmämetodin, koska sillä saadaan osallistujat mahdollisesti näkemään asiat uudella tavalla. Keskenään keskustelu voi tuoda uusia ajatuksia osallistujille, ja heidän mielipiteensä voivat muuttua tilaisuuden edetessä. Kasvotusten tehdyissä haastatteluissa voidaan havainnoida muutakin kuin pelkkää tekstiä, kuten kehonliikkeitä. Ryhmähaastattelulla pystyin säästämään aikaa. Tilaisuuden ohjaaminen antoi myös itselleni uutta kokemusta ja itseluottamusta vastaaviin tilanteisiin.

Haastattelun tavoitteena oli selvittää ammattikorkeakoulun IT-asiantuntijoiden mielipiteet siitä, mitä kaikkia asioita opiskelijoiden tulee itse huomioida käyttäessään BYOD-mallia. Laitteista puhuttaessa haastateltavat tarkoittivat pääosin kannettavia tietokoneita mobiililaitteiden sijaan. Dokumentointimuotona oli muistio. Haastatteluun osallistuneet henkilöt pysyvät anonyymeinä. Seuraavaksi tarkastellaan haastattelussa saatuja tuloksia.

## 4.1 Tietoturvasovellukset opiskelijoiden laitteissa

Ammattikorkeakoulun IT-asiantuntijoiden haastattelussa todettiin, että opiskelijoilla pitäisi olla laitteissaan ainakin ajan tasalla oleva palomuuri sekä haittaohjelmien torjunta-sovellus. Haittaohjelmien torjuntaan tarkoitetuista sovelluksista löytyy lisätietoa ammattikorkeakoulun intranetistä. Jos laite häviää tai tulee varastetuksi, etätyhjennyssovelluksella voidaan paikantaa laite tai

tyhjentää sen data. Lisäksi jokaisella opiskelijalla olisi hyvä olla jonkinlainen varmuuskopiointikäytäntö. Tapoja on monia, mutta tärkeintä on, että varmuuskopiointi tehdään riittävän usein.

## 4.2 Omien laitteiden suojaaminen

Ammattikorkeakoulun IT-asiantuntijoiden haastattelussa todettiin, että kaikki omat laitteet on hyvä olla salasanalla suojattu. Laitteiden lisäksi BIOS (basic input-output system) sekä kovalevy kannattaa suojata salasanalla. Tällä tavoin estetään esimerkiksi boottausjärjestyksen muuttaminen, ja arkaluontoinen data saadaan suojatuksi. Omia salasanoja ei saa säilyttää fyysisesti missään esimerkiksi paperille kirjoitettuna. Myös selaimiin ei suositella käyttäjätunnusten tai salasanojen tallentamista.

Admin-oikeuksia ei suositella käytettävän silloin, kun laitteella suoritettavat toimenpiteet eivät sitä vaadi. Haastateltavat korostivat, että ei kannata käyttää mitään sellaisia teknologioita, mitä ei juuri sillä hetkellä tarvitse. Esimerkiksi bluetooth, webkamera tai mikrofoni kytketään pois päältä, kun niitä ei tarvita. On tärkeää, että opiskelijat perehtyvät omiin laitteisiinsa, jotta he tietävät minkälaisia teknologioita heidän laitteissaan on.

## 4.3 Laitteiden saastumisen ennaltaehkäisy omalla käyttäytymisellä

Ammattikorkeakoulun IT-asiantuntijoiden haastattelussa todettiin, että yleisimmin laitteet saastuvat internetin kautta käyttäjän oman toiminnan kautta. Ainoastaan salattuja verkkoyhteyksiä kannattaa käyttää. Sähköposteissa olevat linkit ja liitetiedostot on hyvä kyseenalaistaa, vaikka ne olisivat tutusta lähteestä peräisin. Sovelluksia suositellaan ladattavan vain luotetuista lähteistä, sillä kolmannen osapuolen sovelluskaupat ovat täynnä haittaohjelmia. Sovellukset ja käyttöjärjestelmä on syytä pitää aina ajan tasalla, jotta havaitut tietoturva-aukot saadaan paikattua.

Opiskelija on itse vastuussa omasta laitteestaan ja sen toiminnasta. Sen vuoksi omien laitteiden lainaamista ei suositella. Esimerkiksi toisen käyttäjän toiminta on voinut saastuttaa laitteen. Kun opiskelija myöhemmin yhdistää laitteensa ammattikorkeakoulun verkkoon, tartunta saattaa lähteä leviämään. Jos laitetta kuitenkin lainataan, kannattaa luoda väliaikainen guest user-tili, jossa on rajatut käyttöoikeudet. Sama kanta lainaamisesta pätee myös muistitikkuihin. Muistitikulla voidaan kaapata laite pelkästään liittämällä se UBS-porttiin. Jos muistitikun turvallisuudesta ei ole varmuutta, sen saa avata ainoastaan suljetussa ympäristössä olevalla laitteella.

### 4.4 Yleisillä paikoilla työskentely

Ammattikorkeakoulun IT-asiantuntijoiden haastattelussa todettiin, että yleisillä paikoilla työskenneltäessä on hyvä ottaa huomioon myös muut ihmiset. Jos työpisteeltä poistutaan edes hetkeksi, näytön lukitsemisen lisäksi laite kannattaa lukita sen hetkiselle työpisteelle fyysisesti. Kirjoittamiseen on syytä kiinnittää huomiota varsinkin silloin, kun kirjoitetaan arkaluontoisia asioita, kuten käyttäjätunnuksia ja salasanoja. Kannettaviin tietokoneisiin on saatavilla myös näyttösuodattimia, jotka rajaavat näytön kuvaa.

### 4.5 Laitteille tehtävät toimenpiteet opiskelun päättyessä

Ammattikorkeakoulun IT-asiantuntijoiden haastattelussa todettiin, että opiskelun päätyttyä kaikki lisenssin vaativat sovellukset, mitkä ammattikorkeakoulun kautta on saatu, täytyy poistaa, jos niihin ei ole erikseen käyttöoikeutta. Jos selaimeen suosituksista huolimatta on tallennettu opintoihin liittyviä tunnuksia tai salasanoja, ne täytyy poistaa. Myös kaikki muiden käyttäjien tuottama materiaali täytyy poistaa.

### 4.6 Muuta haastattelussa ilmenneitä asioita

Ammattikorkeakoulun IT-asiantuntijoiden haastattelussa todettiin, että ammattikorkeakoululla on käytössä muun muassa oma tietoturvapolitiikka ja käyttösäännöt, jotka jokainen opiskelija on lukenut ja hyväksynyt allekirjoituksellaan opiskelun alussa. Ne löytyvät Messistä sekä ammattikorkeakoulun sivuilta. Ylläpitosääntöihin tarvitsee tehdä muutoksia, jotta BYOD-malli tulee olemaan mahdollinen. Tällä hetkellä sääntöjen mukaan omia laitteita ei saa kytkeä ammattikorkeakoulun verkkoon. BYOD-mallin myötä opiskelijan laitteesta tulee osa ammattikorkeakoulun infrastruktuuria, ja näin myös opiskelijasta laitteensa ylläpitäjä.

Suomen lain mukaan ammattikorkeakoulu ei voi pakottaa opiskelijaa hankkimaan jotakin spesifiä laitetta tai sovellusta. Laitteita voidaan ainoastaan suositella. Haastateltavia huoletti tulevien laitteiden suuri skaala sekä väärin konfiguraatioidut laitteet. Huolta aiheutti myös se, että opiskelijat voivat asentaa laitteisiinsa mitä vaan.

Haastateltavat halusivat vielä muistuttaa, että jokaisella opiskelijalla on omat henkilökohtaiset tunnukset ja salasanat. Niitä ei saa luovuttaa kenellekään. Ammattikorkeakoulun järjestelmissä ei saa käyttää samoja salasanoja, jotka ovat muualla käytössä. Opinnäytetyöhön tai projekteihin liittyvät salassapitosopimukset jatkuvat myös opiskelun päätyttyä aivan niin kuin muissakin organisaatiossa. Haastattelussa päädyttiin siihen tulokseen, että suurimmat tietoturvariskit syntyvät käyttäjien tekemistä virheistä ja päivittämättömistä laitteista.

### 4.7 Haastattelun yhteenveto

Ammattikorkeakoulun IT-asiantuntijoille tehdyssä haastattelussa tunnistettiin samat riskit, jotka kirjallisuudesta tuotiin esille. Näiden riskien lisäksi haastattelijoilla tuli mieleen paljon muitakin riskejä. Seuraavassa taulukossa on

lueteltuna haastattelussa tunnistetut tietoturvariskit sekä mahdolliset haitat, jos riskit toetutuvat.

Taulukko 2. Haastattelussa tunnistetut tietoturvariskit ja mahdolliset haitat.

| **Tunnistetut tietoturvariskit** | **Mahdolliset haitat** |
|---|---|
| Puuttuva tai väärin konfiguraatioitu palomuuri | Laitteet ovat alttiina erilaisille hyökkäyksille ja haittaohjelmille. |
| Puuttuva tai päivittämätön haittaohjelmien torjunta-sovellus | Laitteet ovat alttiina erilaisille hyökkäyksille ja haittaohjelmille. |
| Etäyhdistämismahdollisuus mobiililaitteisiin ei aktivoitu | Katoamis- ja varkaustilanteissa ei voi paikantaa mobiililaitetta tai pyyhkiä sen dataa. |
| Puuttuva varmuuskopiointikäytäntö | Yllättävän tapahtuman, kuten laiterikon sattuessa data häviää pysyvästi. |
| Salasanalla suojaamattomat laitteet, BIOS ja kovalevyt | Kuka tahansa voi käyttää laitteita ja pääsee käsiksi laitteissa olevaan dataan. |
| Salasanojen fyysinen säilyttäminen | Ulkopuolinen henkilö voi käyttää tunnuksia, jos saa ne haltuunsa. |
| Salasanojen ja käyttäjätunnusten tallentaminen selaimeen | Ulkopuolinen henkilö voi käyttää tunnuksia, jos saa ne haltuunsa. |
| Pelkkien admin-oikeuksien käyttäminen | Rajattuja käyttöoikeuksia käyttämällä voidaan minimoida esimerkiksi laitekaappauksessa syntyviä vaurioita. |
| Käyttämättömien teknologioiden päällä pitäminen | Esimerkiksi mikrofoni tai webkamera voi joutua kaappauksen |

| | |
|---|---|
| | kohteeksi. Lisäksi teknologiat kuluttavat akkua. |
| Opiskelijan internet käyttäytyminen | Yleisin mahdollinen haitta on haittaohjelmat. |
| Salaamattomien verkkoyhteyksien käyttäminen | Ulkopuolinen henkilö voi tarkkailla kaikkia verkossa olevia tapahtumia. |
| Kolmannen osapuolen sovelluskaupat | Sovellusten mukana tulevat haittaohjelmat. |
| Päivittämättömät käyttöjärjestelmät ja sovellukset | Altistavat laitteet erilaisille tietoturvahyökkäyksille. |
| Laitteiden ja muistitikkujen lainaaminen | Opiskelija on itse vastuussa omista laitteistaan ja niiden turvallisuudesta. Toinen käyttäjä voi toiminnallaan saastuttaa laitteen joko tahallisesti tai tahattomasti. |
| Laitteiden jättäminen vartioimatta | Laitteet saattavat tulla varastetuiksi tai niillä voidaan tehdä ei toivottuja toimenpiteitä. |
| Saman salasanan käyttäminen eri tunnistamisissa | Salasanan vaarantuessa sitä voidaan käyttää useissa eri tunnistamisissa. |

# 5 YHTEENVETO

Opinnäytteen tavoitteena oli selvittää opiskelijan näkökulmasta erilaisia BYOD-mallin tietoturvariskejä sekä mitä asioita BYOD-mallia käytettäessä tulee ottaa huomioon. BYOD-malli ja sen tuomat tietoturvariskit ovat aiheena todella laaja kokonaisuus. Tämän suuruiseen työhön oli mahdotonta saada syvällisesti sisällytettyä kaikki asiat. Mielestäni kuitenkin onnistuin saamaan työhön tärkeimpiä BYOD-mallin tietoturvariskejä, mitä opiskelijoiden tulee huomioida. Tämän opinnäytteen luettuaan opiskelijat saavat perusvalmiudet kohti turvallisempaa BYOD-ympäristöä.

Mobiililaitteiden yleistyessä jokainen organisaatio joutuu väistämättä siirtymään BYOD-malliin jollain tavalla. BYOD-mallia hyödynnetään käyttämällä erilaisia teknologioita, kuten työpöytävirtualisointia ja verkkosovelluksia. Hyvin toteutetulla BYOD-ratkaisulla voidaan saavuttaa suuria hyötyjä ja etuja. Turun ammattikorkeakoulussa kustannuksia saadaan pienennettyä, kun voidaan luopua suurista tietokoneluokista. Laitteistoa ei tarvitse koko ajan uusia ja ylläpito tulee olemaan halvempaa. Melkein kaikilla opiskelijoilla on jo ennestään käytössään kannettavia ja muita mobiililaitteita. Yleensä laitteet ovat uudempia, kuin koulun tarjoamat laitteet. Itse hankitulla laitteella on mukavampi työskennellä, kun se on juuri sellainen, millaisen itse haluaa. Laitteiden ollessa omia niillä voi työskennellä paikasta riippumatta. Omista laitteista pidetään myös parempaa huolta. Näin ollen ilkivaltatapaukset pienenevät.

Tietoturvauhat muuttuvat jatkuvasti. Tästä syystä myös teknisten vastatoimien metodeja pitää muuttaa. Opiskelijat voivat vaikuttaa lähinnä ennaltaehkäisy- ja reaktiovaiheeseen. Tärkeintä on, että käytettävät laitteet ja järjestelmät ovat ajan tasalla, ja laitteiden tietoturva ja -suoja ovat riittävällä tasolla. Myös mahdollisimman monimutkaisten salasanojen käyttö edesauttaa ennaltaehkäisyä.

Opinnäytetyötä voisi jatkaa syventymällä BYOD-mallin tietoturvariskeihin. Opiskelijoiden lisäksi työssä voitaisiin tutkia tietoturvariskejä kaikkien käyttäjien

näkökulmasta. Tämä tietysti vaikuttaisi opinnäytteen otsikointiin. Opinnäytteen pohjalta opiskelijoille voisi suunnitella jonkinlaisen tietoturvakäyttöoppaan.

# LÄHTEET


Assing, D. & Calé, S. 2013. Mobile Access Safety: Beyond BYOD. Wiley-ISTE.

Barbier, J.; Bradley, J.; Macaulay, J.; Medcalf, R. & Reberger, C. 2012. BYOD and Virtualization Top 10 Insights from Cisco IBSG Horizons Study. Viitattu 8.4.2016 http://www.cisco.com/c/dam/en_us/about/ac79/docs/BYOD.pdf

Brodin, M. 2016. BYOD VS. CYOD – WHAT IS THE DIFFERENCE? Viitattu 20.7.2016 http://his.diva-portal.org/smash/get/diva2:920380/FULLTEXT01.pdf

Disterer, G. & Kleiner, C. 2013. BYOD Bring your own device. Viitattu 20.7.2016 http://www.sciencedirect.com/science/article/pii/S221201731300159X#

Endler, M. 2013. Desktop Virtualization vs. BYOD, Windows Worries. Viitattu 21.4.2016 http://www.informationweek.com/applications/desktop-virtualization-vs-byod-windows-worries/d/d-id/1111074?

Evans, D. 2015. What is BYOD and why is it important? Viitattu 5.4.2016 http://www.techradar.com/news/computing/what-is-byod-and-why-is-it-important--1175088

IBM 2016. What is bring your own device? Viitattu 20.3.2016 http://www.ibm.com/mobilefirst/us/en/bring-your-own-device/byod.html

ITGCT 2015. How DaaS improves Business BYOD Programs. Viitattu 23.6.2016 https://www.itgct.com/how-daas-improves-business-byod-programs/

Jackson, W. 2013. Just what does NIST consider a mobile device? Viitattu 20.4.2016 https://gcn.com/articles/2013/06/27/nist-mobile-device-definition.aspx

Landoll, D. 2011. The Security Risk Assessment Handbook. 2. painos. Boca Raton: Taylor & Francis Group.

La Piedra, J. 2002. The Information Security Process Prevention, Detection and Response. Viitattu 28.7.2016 https://www.giac.org/paper/gsec/501/information-security-process-prevention-detection-response/101197

Marczak, M. & Sewell, M. 2016. USING FOCUS GROUPS FOR EVALUATION. Viitattu 19.9.2016 http://ag.arizona.edu/sfcs/cyfernet/cyfar/focus.htm

Prashant, K.; Arnab, G. & Shashikant R. 2013. Bring your own device (BYOD): Security risks and mitigating strategies. Viitattu 23.3.2016 http://www.jgrcs.info/index.php/jgrcs/article/view/654/477

Swanepoel, R. 2015. BYOD: ARE YOU MISSING THE BOAT? Viitattu 11.10.2016 http://search.proquest.com.ezproxy.turkuamk.fi/docview/1687838905/fulltextPDF/FF528484904B4838PQ/1?accountid=14446